Prof. Dr. Urs Hartl
Martin Brandenburg

13. Übungsblatt

Abgabetermin: Mo, 21.1.13, 12 Uhr

1. Sei $\mathrm{char}(k) \neq 2$ und seien $a, b \in k$, $\tilde{a} := -2a$, $\tilde{b} := a^2 - 4b$ mit $b \neq 0$, $\tilde{b} \neq 0$. Seien E und $\tilde{E}$ durch die Weierstraß-Gleichungen

$$E: \ y^2 = x^3 + ax^2 + bx \qquad \text{und} \qquad \tilde{E}: \ \tilde{y}^2 = \tilde{x}^3 + \tilde{a}\tilde{x}^2 + \tilde{b}\tilde{x}$$

gegeben. Betrachten Sie die Isogenien:

$$\varphi : E \to \tilde{E}, \quad \varphi^*(\tilde{x}) = \tfrac{y^2}{x^2}, \quad \varphi^*(\tilde{y}) = \tfrac{y(x^2-b)}{x^2}$$

$$\psi : \tilde{E} \to E, \quad \psi^*(x) = \tfrac{\tilde{y}^2}{4\tilde{x}^2}, \quad \psi^*(y) = \tfrac{\tilde{y}(\tilde{x}^2-\tilde{b})}{8\tilde{x}^2}$$

   (a) Zeigen Sie, dass φ und ψ separabel sind. Hinweis: $\varphi^*\omega \neq 0$.

   (b) Bestimmen Sie $\ker\varphi$, $\ker\psi$, $\deg\varphi$ und $\deg\psi$.

   (c) Zeigen Sie $\psi \circ \varphi = [2] : E \to E$ und $\varphi \circ \psi = [2] : \tilde{E} \to \tilde{E}$.

   (d) Sei $P \in E(k^{\mathrm{alg}})$ mit $\varphi(P) \in \ker\psi$, $\varphi(P) \neq 0$, z.B. $P = (\alpha : 0 : 1)$ für $\alpha \in k^{\mathrm{alg}}$ mit $\alpha^2 + \alpha a + b = 0$. Zeigen Sie

$$E[2](k^{\mathrm{alg}}) = \{0, P\} \oplus \ker\varphi \cong (\mathbb{Z}/2)^2.$$

(8 Punkte)

2. Finden Sie integre Gruppenschemata E, E' über k mit neutralen Elementen $0 \in E(K)$ und $0' \in E'(k)$, sowie einen Morphismus $\varphi : E \to E'$ von k-Schemata, der zwar $\varphi(0) = 0'$ erfüllt, aber kein Homomorphismus von Gruppenschemata ist. Insofern stellt Satz 2.4.4 also eine besondere Eigenschaft von elliptischen Kurven, bzw. eigentlichen integren Gruppenschemata dar. *(2 Punkte)*

3. Die elliptische Kurve E über $\mathbb{F}_2$ sei gegeben durch die Weierstraß-Gleichung $y^2 + y = x^3 + a_6$ mit $a_6 \in \mathbb{F}_2$.

   (a) Zeigen Sie $[2] = \varphi \circ \mathrm{Fr}_4$ und $\widehat{\mathrm{Fr}}_2 = \varphi \circ \mathrm{Fr}_2$ für geeignetes $\varphi \in \mathrm{Aut}(E)$.

   (b) Bestimmen Sie damit $E[2](k^{\mathrm{alg}})$ (vgl. Aufgabe 3, Blatt 12).

   (c) Berechnen Sie $\deg(1 - \mathrm{Fr}_{2^r})$ für $r = 1, \ldots, 8$ mit Hilfe von $\widehat{\mathrm{Fr}}_{2^r}$. Überprüfen Sie das Ergebnis, in dem Sie direkt $\#E(\mathbb{F}_{2^r})$ bestimmen. *(6 Punkte)*

4. $\star$ Finden Sie heraus, wo Sie im Alltag mit elliptischen Kurven in Berührung kommen. Sie werden es nicht glauben. Ein mögliches Stichwort lautet *ECC*.

5. Welche Zusammenhänge, Details, Inhalte oder Fragen sollen in der Übung am 23.1. besprochen werden? *(2 Punkte)*